

# Comment on "A strong provably secure IBE scheme without bilinear map" by M. Zheng, Y. Xiang and H. Zhou [J. Comput. Syst. Sci. **81** (2015), 125–131]

Damien Vergnaud

*École normale supérieure – 45 rue d’Ulm – 75230 Paris Cedex 05 France*

---

## Abstract

Zheng, Xiang and Zhou published in Journal of Computer and System Sciences in 2015 a “strong provably secure IBE scheme without bilinear map”. In this note, we provide two very simple attacks on their scheme.

*Keywords:* Cryptanalysis, Identity-based encryption

---

## 1. Introduction

Identity-based cryptography was introduced by Shamir in [7]. It aims to simplify key management by removing the need for digital certificates used in traditional public-key infrastructures. In such systems, users’ public keys are public identifiers (e.g. email addresses) and the matching private keys are derived by a trusted party (called the private key generator). The first practical constructions for Identity-Based Encryption (IBE) was proposed by Boneh and Franklin [1] and relies on the existence of efficient bilinear maps on specific groups. Since then, a large body of work has been devoted to the design of schemes with additional properties or relying on different algorithmic assumptions (*e.g.* [4, 5]).

It is desirable for cryptosystems based on the discrete logarithm problem to be constructed without relying on bilinear maps. In [8], Zheng, Xiang and Zhou proposed a “strong provably secure IBE scheme without bilinear map”. They claimed that their proposal achieves the so-called IND-ID-CCA security assuming the classical computational Diffie-Hellman assumption. In this note, we show that this claim is wrong and we show two very simple polynomial-time attacks on their scheme: the first one is against the one-wayness of the scheme and uses only the public parameters and the second one is a key-recovery attack that requires a few extraction queries (*i.e.* users’ private keys for chosen identities).

---

*Email address:* `damien.vergnaud@ens.fr` (Damien Vergnaud)

## 2. Cryptanalysis of Zheng-Xiang-Zhou scheme

**Description of Zheng-Xiang-Zhou scheme.** Let  $(\mathbb{G}, +)$  be a group of prime-order  $q$  (following [8], we use additive notation for the group law). Given two generators  $P$  and  $Q = [a]P$  of  $\mathbb{G}$ , the private key generator picks uniformly and independently at random  $h$  scalars  $r_1, \dots, r_h$  in  $\mathbb{Z}_q^*$  for some integer  $h$ . It publishes the points  $[r_i]P$  and  $[r_i]Q$  for  $i \in \{1, \dots, h\}$  as the public parameters and keeps the values  $r_i$  for  $i \in \{1, \dots, h\}$  as its secret key.

From a user public-key ID, a binary string of length  $h$  is derived using a hash function  $H_{id}$  whose security properties are not specified in [8]. Given this binary string  $H_{id}(\text{ID}) = a_1 \dots a_h \in \{0, 1\}^h$ , the user secret key is derived by the private-key generator as  $\text{SK}_{\text{ID}} = \sum_{i=1}^h a_i \cdot r_i \bmod q$  and we denote  $P_{\text{ID}} = \sum_{i=1}^h [a_i r_i]P$  and  $Q_{\text{ID}} = \sum_{i=1}^h [a_i r_i]Q$  two elements in  $\mathbb{G}$  that can be publicly computed from ID and the public parameters.

The encryption algorithm uses two additional hash functions  $H_1 : \mathbb{G} \rightarrow \{0, 1\}^k$  and  $H_2 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$  modelled as random oracles in the (flawed) security analysis. Given a message  $m \in \{0, 1\}^k$  and an identity ID, the encryption algorithm picks at random  $\sigma \in \{0, 1\}^k$ , computes  $r = H_2(\sigma, \text{ID})$ , and outputs  $c = ([r]P, H_1([r]P_{\text{ID}}) \oplus \sigma, H_1([r]Q_{\text{ID}}) \oplus m, H_2(\sigma, \text{ID}))$  as the ciphertext. The decryption algorithm is described in [8] (but is not relevant for the attacks).

**Description of the attack on the one-wayness.** Given a ciphertext  $c = (c_1, c_2, c_3, c_4)$ , an adversary can trivially recover  $r$  as  $c_4 = H_2(\sigma, \text{ID})$  and then the associated plaintext as  $c_3 \oplus H_1([r]Q_{\text{ID}})$ . This attack is actually more efficient than the decryption algorithm described in [8]. It comes from the use of a very poor redundancy scheme in order to achieve CCA-security that actually weakens the security of the IBE scheme. Even if this can be easily fixed, our second attack demonstrates that the scheme is broken beyond repair.

**Description of the key-recovery attack.** For the key-recovery attack, we consider an adversary that is allowed to query only  $h$  times the *Extract* algorithm in order to obtain secret keys of users of its choice (and in particular is legitimate in the IND-ID-CCA security game describe in [8]).

Even if  $H_{id}$  is a strong cryptographic hash function or a random oracle (see [3]), a very simple attack can be mounted. The adversary can simply pick iteratively identities  $\text{ID}_j$  for  $j \in \{1, \dots, h\}$  at random such that the matrix  $A_t = (a_i^{(j)})_{i \in \{1, \dots, h\}, j \in \{1, \dots, t\}}$  is of rank  $t$  in  $\mathbb{Z}_q^{h \times t}$  for  $t \in \{1, \dots, h\}$  (where  $H_{id}(\text{ID}_j) = a_1^{(j)} \dots a_h^{(j)}$  for  $j \in \{1, \dots, h\}$ ).

If  $H_{id}$  is a random oracle, then  $A_h$  is a random binary matrix over  $\mathbb{Z}_q$ . It is well-known that a random  $(h \times h)$ -matrix over  $\mathbb{Z}_q$  where each entry is chosen independently and uniformly at random in  $\mathbb{Z}_q$  is non-singular with at least some constant probability [6]. The problem is less studied for random binary matrices over finite fields but one can easily prove (e.g. [2, Lemma 4]) that if one concatenates a random binary vector of length  $h$  to a binary  $(h \times n)$ -matrix of rank  $r < h$ , then the rank of the resulting  $(h \times n + 1)$ -matrix is  $r + 1$  with probability at least  $1/2$ . Therefore, by picking on average only  $2h$  identities ID, the adversary can construct an invertible matrix  $A_h$  as described and it

can recover the secret key vector  $(r_1, \dots, r_h)$  as  $(\text{SK}_{\text{ID}_1}, \dots, \text{SK}_{\text{ID}_h}) \cdot {}^t(A^{-1})$  (by quering the *Extract* algorithm on the  $h$  identities  $\text{ID}_j$  for  $j \in \{1, \dots, h\}$ ).

## References

- [1] D. Boneh and M. Franklin, *Identity-Based Encryption from the Weil Pairing*, SIAM J. Comput. **32** (2003), no. 3, pp. 586–615
- [2] N. H. Bshouty and H. Mazzawi, *On Parity Check  $(0,1)$ -Matrix over  $\mathbb{Z}_p$* , Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms (D. Randall, ed.), ACM-SIAM, 2011, pp. 1383–1394.
- [3] M. Bellare and P. Rogaway, *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols*, Proceedings of the First ACM Conference on Computer and Communications Security (D. Denning, R. Pyle, R. Ganesan, R. Sandhu, and V. Ashby, eds.), ACM Press, 1993, pp. 62–73.
- [4] C. Cocks, *An Identity Based Encryption Scheme Based on Quadratic Residues*, Cryptography and Coding, 8th IMA International Conference (B. Honary, ed.), Lect. Notes Comput. Sci., vol. 2260, Springer, 2001, pp. 360–363
- [5] C. Gentry, C. Peikert and V. Vaikuntanathan. *Trapdoors for hard lattices and new cryptographic constructions*, Proceedings of the 40th Annual ACM Symposium on Theory of Computing (C. Dwork, ed.), ACM, 2008, pp. 197–206.
- [6] G. Landsberg, *Über eine Anzahlbestimmung und eine damit zusammenhängende Reihe*, J. Reine und Angewandte Math. 111 (1893), 87–88.
- [7] A. Shamir, *Identity-Based Cryptosystems and Signature Schemes*, Advances in Cryptology - Crypto '84 (G. R. Blakley and D. Chaum, eds.), Lect. Notes Comput. Sci., vol. 196, Springer, 1985, pp. 47–53.
- [8] M. Zheng, Y. Xiang and H. Zhou, *A strong provably secure IBE scheme without bilinear map*, J. Comput. Syst. Sci. **81** (2015), pp. 125–131.